The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 4 || Pages || PP -67-70|| 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

A Comparitive Analysis Of Steganography Techniques

[1]Kirandeep , [2]Dr.Raman Maini
[1]*Department of Computer Engineering, University College of Engineering, Punjabi University, Patiala, India*
[2]*Professor, Department of Computer Engineering, University College of Engineering, Punjabi University, Patiala, India.*

----------ABSTRACT----------
With the increase in rate of unauthorized access and attacks security of confidential data is important. Now a day Cryptography and Steganography are the secure communication media for security purposes. This paper focuses on quantitative comparision of steganography technique such as improved LSB technique for RGB images, pattern based steganography technique and raster scan technique. The simulation has been done on MATLAB 2013 using 20 images and output of few has been shown in this paper. It has been concluded that the on the basis of various factors such as quantitative measures of the three techniques, pattern based steganography technique is the best among the other techniques w.r.t to security , irrespective of the fact that this technique has low capacity.
Keyword : *Steganography, Cryptography, Security***.**
Date of Submission: 13 April 2016 Date of Accepted: 24 April 2016

I.INTRODUCTION

The popularity of internet and its technologies increases day by day and so are the threats to the security of our information transmitted through the internet. The unauthorized or illegal access of the data or tampering of data is very high. In order to provide security of data being accessed by unauthorized people, information hiding is required [1].

Steganography is basically an art of passing information through original files in such a way that the existence of the message is unknown. The Steganography term is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" and literally means "Cover writing". In this technique message is hidden in a way in which no one can detect the existence of the message except the sender and the receiver. The main goal of the steganography technique is to hide the data in such a way that eavesdroppers cannot detect the message.
There are various types of steganography:
1.Text steganography
2.Image steganography
3. Audio video steganography
4. Protocol steganography

In Text steganography, the secret message is hidden in every nth letter of every word of a text message. In Image steganography the secret message is hidden in the pixels of the image and they are very popular cover objects for steganography.Now, in Audio Video steganography , the secret message is hidden in audio or video files and the technique of masking is used in it.The Protocol steganography is the one in which information is embedded within the messages and network control protocols used in network transmission.
In this paper,Section 2 describes elements of steganography, section 3 and 4 describes parameters and various techniques of steganography respectively.Section 5 and 6 defines results and conclusion .Other goal of steganography is to communicate in a complete secure undetectable manner [2].

II. ELEMENTS OF STEGANOGRAPHY

The three basic elements of steganography i.e cover object,message and stego object, of which steganography is composed of ,are defined as follows:

1. Cover Object

In Steganography the cover object, in which Secret Message is to be hidden. The cover objects are anything like images, audio, videos, text. The most used cover object for hide information is image.

2. Message

In the Steganography the Secret message, the message hides in cover image. The Secret message like images, text messages etc.

3. Stego Object

The Stego object generated after hiding the secret message in cover image. After that the Stego Object is transmitted. At receiver side processing is done on Stego object to retrieve message from it.

III. PARAMETERS OF STEGANOGRAPHY

In Steganography techniques a message embed inside a cover image. There are many parameters which affects the steganography techniques. The parameters are as follows:

1.Capacity

The capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system.

2.Robustness

Robustness refers to the ability of the embedded data to remain intact if the system undergoes transformation like linear and non-linear filtering, addition of random noise, rotation, scaling and compression, sharpening or blurring, lossy compression.

3.Undetectable

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images is drawn. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image.

4.**Invisibility (Perceptual Transparency)**

The concept of Invisibility based on the properties of the human visual system. The embedded information is imperceptible if an average human is unable to distinguish between carriers that contain hidden information and others do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover.In extreme secure communications, if a hacker senses that there is some distortion that shows the presence of hidden data in a stego-image, the steganographic encoding has failed even if the message is not extracted. It is one of the important parameter.

5.SECURITY

The embedded algorithm is to be secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key [3].

6.INDEPENDENT OF FILE FORMAT

The most powerful Steganographic algorithms thus possess the ability to embed information in any type of file.

IV.VARIOUS EXISTING TECHNIQUES

There are various techniques proposed in image steganography in order to hide the secret message.The efficiency of a technique is described by the quality of out image as well its level of security.Among all of them,three techniques have been described and they are as follows:

4.1 Improved LSB based Image Steganography Technique for RGB Images[4]

The LSB technique for color images is preferred because of its simplicity, easily understandable to the user and the easy way of hiding information by replacing the least significant bit of each pixel. But when we hide more data into an image by using LSB, image resolution is changed at the pixels where the data is hidden because it induces noise. Also,security of information is less because it can be easily detected by someone by simply recovering the least significant bit of the pixel.So this technique focusses on removal of noise so as to provide better quality of the image after hiding the data in it.It hides the message bits into the three planes of the colour image after bit plane slicing.This is done in a way so that it induces minimum noise in the stego image.

In this technique,firstly cover image is read and the image is bit sliced into three places i.e Red ,Green and Blue. After that the images to be hidden ,are read. Further,images are selected one by one to be hidden in Red,Green and Blue planes. Then the bits of Cover image are replaced in order of 2:2:4 of the LSB in three planes (i.e. Red, Green and Blue planes) with the bits of message image.The reconstructed image is displayed after the hiding process.

4.2 An Innovative Approach for Pattern Based Image Steganography[5]:

This technique allows the sender to embed the secret message into the hierarchically divided subsections. It uses a pattern of ‘Z’ and ‘alpha’ in an image in order to increase the security.

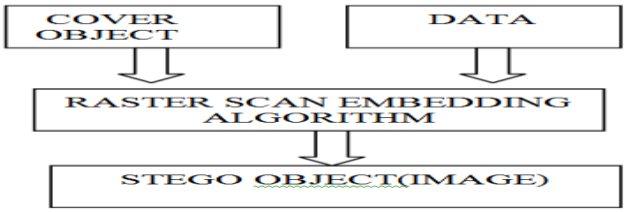
First of all, the input cover image is divided into 25×25 non overlapped windows. Then further each window is divided into 5×5 subsections. Then among them, the sub sections will be selected based on the pattern 'Z’. Next, in the second stage, within each selected 5×5 sub section, the pixels will be selected based on the pattern ‘alpha’. Finally,in the selected pixels , least significant bit is used to hide the secret message.

This technique shows its efficiency w.r.t various measures viz., Mean Square Error(MSE), Mean Absolute Error(MAE), Root Mean Square Error(RMSE),Peak Signal to Noise Ratio(PSNR),Signal to Noise Ratio(SNR).

4.3 Raster Scan Technique for Secure Communication in Steganography[6]:

In this technique,data is firstly encrypted and then hidden using raster scan principle.It is almost similar to the raster scan technique to displaying an image on CRT display.

In this,firstly cover image is read and converted to binary format.After that encrypted data is hidden in the cover image using raster scan principle i.e by doing XORing of the cover image with data bits. Next, Mean Square Error is calculated by comparing the stego image with cover image.



FLOW CHART OF RASTER SCAN ALGORITHM
Fig.1

	ORIGINAL IMAGE	IMPROVED LSB TECHNIQUE [4]	PATTERN BASED METHOD [5]	RASTER SCAN TECHNIQUE [6]
1				
2				
3				

Table 1

V.RESULTS AND DISCUSSIONS

The three techniques have been simulated in MATLAB 2013 using 20 images and results of few has been shown in Table 1 . Three images Lena.jpg, Fruits.jpg and Person.jpg have been used for Pattern based technique, LSB technique and raster scan technique and the output images have been shown in the table. Comparision between the three techniques has been done on the basis of various other parameters such as security, capacity etc and is shown in Table 2.

Table 2: Comparision of Three techniques:

Technique	MSE	PSNR
For Lena.jpg		
Improved LSB technique [4]	0.06	59.81dB
Pattern based method [5]	0.016	65.89dB
Raster scan technique[6]	0.0606	60.30dB
For Fruit.jpg		

Table3: Quantitative Results: On the basis on MSE, PSNR

Technique	MSE	PSNR
For Lena.jpg		
Improved LSB technique [4]	0.06	59.81dB
Pattern based method [5]	0.016	65.89dB
Raster scan technique[6]	0.0606	60.30dB
For Fruit.jpg		
Improved LSB technique [4]	0.067	59.81dB
Pattern based method [5]	0.0167	65.89dB
Raster scan technique [6]	0.067	60.30dB
For Person.jpg		
Improved LSB technique [4]	0.0679	59.81dB
Pattern based method [5]	0.0167	65.89dB
Raster scan technique [6]	0.60	60.30dB

So, According to quantitative results, the technique with minimum MSE and maximum PSNR is the best. In digital image processing, technique with PSNR value 30 dB is acceptable .Among the above discussed techniques, Pattern based method is better because this technique has minimum MSE and maximum PSNR for all the images. Pattern based technique has low capacity than raster scan technique and LSB based technique because of the reason that in this technique, the work is done on the pixels covered by 'alpha' and 'Z' pattern only. Raster scan technique and improved LSB technique has more capacity than pattern based steganography technique as they work on all the pixels of the image but they are less secure but security in Pattern based steganography technique is high because of 'Z' and 'alpha' patterns.This technique is best because of the concept that it uses very high security mechanism of 'Z' and 'alpha' pattern in which the data is embedded. Also high invisibility ,due to the fact that because of high security it difficult for anyone to detect a message is being sent , high robustness as it is not prone to attacks easily and high security are parameters that make this method best among all other steganography techniques.

This is the reason why mean square error is least in this technique.

VI. CONCLUSION

In this paper an overview of steganography and its parameters has been given.. Comparison between the three techniques has been discussed on the basis of its quantitative nature. It has been concluded that pattern based technique is best among them on the basis of security irrespective of the fact that it has low capacity This is because of the reason that this technique uses 'Z' and 'Alpha' patterns i.e two level security system.

REFERENCES

[1] Dr. Sudeep D. Thepade, Smita S. Chavan, "Consine, Walsh and Slant Wavelet Transform for Robust Image Steganography", Tenth International Conference on Wireless and Optical Communication Networks, pp. 1-5, July 2013.

[2] Himanshu Gupta , Prof Ritesh Kumar , Dr. SoniChanglani "Enhanced Data Hiding Capacity using LSB-Image Steganography Method" International Journal of Emerging Technology and Advanced Engineering, Vol 3,June 2013.

[3] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, "Comparison of different techniques for Steganography in images", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 2, February 2014

[4] Amritpal singh, Harpal singh "An Improved LSB based Image Steganography Technique for RGB Images"IEEE ,2015.

[5] M. Radhika Mani, V. Lalithya, P. Swetha Rekha, "An innovative approach for pattern based image steganography", IEEE, 2015

[6] Yogita Birdi , Harjinder Singh "Raster Scan Technique for Secure Communication in Steganography" IJAREEIE, Vol. 4, Issue 6, June,2015.

[7] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (UERA), Vol. 2, Issue 3, pp. 338-34 1,2012.

[8] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (IClCT), pp. 749- 755, Feburary 2014.

[9] Jasleen Kour, Deepankar Verma, "Steganography Techniques- A review paper", International Journal of Engineering Research in Management and technology, vol. 3, pp. 132-135, may 2014.

[10] Gunjan Chugh, Rajkumar Yadav, and Ravi Saini, "A new image steganograpgic approach based on Mod factor for RGB images", International Journal of signal processing, image processing, and pattern recognition, vol. 7, pp. 27-44, 2014.

[11] Md. Khalid Imam Rahmani, Kamiya Arora, and Naina Pal, "A crypto-Steganography: A Survey", International Journal of Advanced Computer Science and application, vol.5, 2014

[12] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology (/JAST), Vo1.54, pp. 1 13- 123, May 2013.